Signing on the Dotcom Line

National Security

The patent-pending INL digital signature process allows a person to "sign" information that exists in hundreds of different locations in computer databases, not in just a single file.

Smart Card Technology

Digital signatures and databases sign away paperwork

Smart cards look and feel like simple credit cards. But they act like tiny computers. Idaho National Laboratory is using smart cards in a novel digital signature process developed for databases.

A digital or electronic signature gives personal approval through computers and data lines rather than signing a piece of paper with pen and ink. Electronic signatures, from simple image scans to encrypted programs, are being developed the world over. In October 2000, the U.S. enacted an electronic signature law that made digital signatures legally acceptable.

The nuclear age meets the information age

Developed for managing and shipping nuclear waste, the INL digital signature represents one of the most complex digital signatures yet. The combination of government regulations, transportation requirements and environmental concerns makes shipping waste a monumental paper producer, as much as one thousand pages per drum of waste. The INL electronic waste management process and its digital signature make shipping waste all but paperless.

The patent pending INL process allows a person to "sign" information that resides in hundreds of different locations on computer databases, unlike other

Continued next page

INL Idaho National Laboratory

Continued from previous page

digital signatures that sign only one file. The compiled information is sent to a microprocessor chip on the smart card where it is tightly compressed and encrypted to create the signature. The information and the signature are inseparable.

Trucking along the internet superhighway

Similar to those commonly found on other smart cards, the INL electronic signature is made up of private and public keys. Mathematical encryption formulas create public and private keys simultaneously — the private key signs electronic documents and the public key proves the signature's authenticity. The private key stays in the smart card with the signer and the public key is available wherever the signature needs to be verified.

After INL employees insert their smart card and PIN into the electronic waste management system, they can approve forms as with any electronic system. However, the information they are approving is assembled from thousands of data points within the management system, such as from databases of transportation and federal government requirements. After signing, the information is compressed and encrypted entirely on their card's microprocessor.

Keeping tabs on data

For INL employees managing and shipping nuclear waste, the electronic waste management system also keeps track of any changes to the information the employee originally signed off on. Any changes are flagged by the system for the employee to clarify, much like contract changes require the signer's initials.

The cryptographic algorithms guarantee each private key has one and only one public key. The "key pair" can be revoked or set to expire at any time, but if a private key is revoked and no longer valid, the public key will still recognize the historical signature.

For more information

Wayne Austad
208-526-5423
Wayne.Austad@inl.gov

The INL is a U.S. Department of Energy National Laboratory

Managing and shipping nuclear waste is a monumental paper producer. The digital signature process not only makes these waste management activities all but paperless, it also helps ensure the integrity of the information.